REMARKS

Claims 1-27 are all the claims presently pending in the application.

Claim 8 is amended merely to provide proper antecedent basis, thereby overcoming the rejection of claims 8 and 15-19 under 35 U.S.C. § 112, second paragraph, as set forth below, and not for distinguishing the invention over the prior art, narrowing the claims or for any statutory requirements of patentability. Further, Applicants specifically state that no amendment to any claim herein should be construed as a disclaimer of any interest in or right to an equivalent of any element or feature of the amended claim.

Claims 8 and 15-19 stand rejected under 35 U.S.C. § 112, second paragraph. Claims 1-27 stand rejected on prior art grounds.

With respect to the prior art rejections, claims 1, 3-7, 9, 13, 24, 25, and 27 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Leppek (U.S. Patent No. 5,933,501) in view of Maillard et al. (U.S. Patent No. 6,466,671; hereinafter "Maillard"). Claims 2, 10-12, 14, 23, and 26 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Leppek in view of Maillard, and further in view of Perlman et al. (U.S. Patent No. 5,261,002; hereinafter "Perlman"). Claims 8, 15-18, and 20-22 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Leppek in view of Maillard, and further in view of Schneier, "Applied Cryptography: Protocols, Algorithms, and Source Code in C", Second Edition, pps. 466-474 (hereinafter, "Schneier"). Claim 19 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Leppek in view of Maillard, and further in view of Schneier, and further in view of Perlman.

These rejections are respectfully traversed in the following discussion.

I. THE CLAIMED INVENTION

The claimed invention relates to a method and system for producing wise cards.

In an illustrative, non-limiting embodiment of the invention, as defined by independent claim 1, a method of preventing counterfeiting of a smart card includes providing a smart card with a cryptographic structure for authorizing the smart card which cannot be accessed completely by a predetermined small number of readings, wherein said cryptographic structure can be built only by whoever emits the card or an agent thereof.

In another exemplary embodiment of the invention, as defined by independent claim 24, a method of preventing counterfeiting of a smart card includes providing a smart card such that none of confidential information and a cryptographic key for authorizing the smart card, is carried on the smart card, reading said card by a reader such that in each reading, said reader reads only a predetermined small amount of information which makes the card unique.

In another exemplary embodiment of the invention, as defined by independent claim 26, a system for preventing cloning of a smart card includes a smart card such that a cryptographic structure for authorizing the smart card is not carried on the smart card, and a reader for reading the smart card and including a database for linking to a network and being updated periodically with a list of unauthorized smart cards, wherein said cryptographic structure is kept secret by whoever emits the card or an agent thereof.

In another exemplary embodiment of the invention, as defined by independent claim 27, a signal-bearing medium tangibly embodying a program of machine-readable instructions executable by a digital processing apparatus to perform a method for preventing counterfeiting and cloning of smart cards includes providing a smart card with a cryptographic structure for authorizing the smart card which cannot be accessed completely by a predetermined number of

readings, wherein said cryptographic structure can be built only by whoever emits the card or an agent thereof.

In conventional methods and systems, counterfeiting/duplication is not rendered difficult since confidential information is carried on the card and an unscrupulous person may find the information simply by looking at or reading the energy construction inside of the card. That is, with a plurality of readings of the card, the information held within the card can be easily detected (e.g., see specification at page 3, line 19, to page 4, line 2).

The claimed invention, on the other hand, complements the conventional smart-card-type of security, which is often all carried on the card itself, by providing extra protection depending on cryptography, with the cryptographic structure (e.g., a key) not being carried by the card and which cannot be accessed completely by a predetermined small number of readings. Moreover, the cryptographic structure can only be built by whoever emits the card or the agent thereof (e.g., see specification at page 4, lines 9-13).

The claimed invention, in addition to preventing the creation of false cards different from the legitimate ones, also prevents the fabrication of clones of a given legitimate smart card. That is, the present invention also provides a mechanism of protection designed to prevent and/or discourage both copying and creation of new cards (e.g., see specification at page 4, lines 14-17).

I. CLAIM REJECTION UNDER 35 U.S.C. § 112

Claims 8 and 15-19 stand rejected under 35 U.S.C. § 112, second paragraph, as allegedly being indefinite. As mentioned above, claim 8 is amended to provide proper antecedent basis, thereby overcoming the rejection under § 112. Therefore, the Examiner respectfully is requested to withdraw this rejection.

II. THE PRIOR ART REJECTIONS

A. Claims 1, 3-7, 9, 13, 24, 25, and 27 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Leppek in view of Maillard. Applicant submits, however, that there are elements of the claimed invention which are neither taught nor suggested by Leppek or Maillard, alone or in combination, and therefore, Applicants respectfully traverse this rejection.

First, the Examiner alleges that Leppek discloses "*a method for preventing counterfeiting and cloning of smart cards*" (see Office Action at page 3, numbered paragraph 6).

However, as the Examiner acknowledges, Leppek does not disclose or suggest a smart card (see Office Action at page 4, line 4).

Moreover, the Examiner alleges that Leppek discloses "*providing a smart card with a cryptographic structure for authorizing the smart card which cannot be accessed completely by a predetermined number of readings*", as allegedly disclosed at column 4, lines 8-66, and the Abstract of Leppek.

However, as mentioned above and as acknowledged by the Examiner, Leppek clearly does not disclose or suggest a smart card (see Office Action at page 4, line 4).

Thus, for at least these reasons, Applicant respectfully submits that the Office Action clearly has mischaracterized Leppek as disclosing a smart card.

On the other hand, the Examiner alleges that Maillard makes up for the deficiencies of Leppek by disclosing a smart card used in communication systems.

The Examiner alleges that it would have been obvious "*to implement the teachings of Leppek onto a smart card, as taught by Maillard et al., because smart cards are small, easy to use mediums (sic) for encryption*" and because "*a method which prevents a footprint or playback*

attack (sic) from being performed by an intruder would help spread the acceptance of smart cards used in technology" (see Office Action at page 4, lines 8-15; emphasis added).

Applicants respectfully submit, however, that it would not have been obvious to modify Leppek based on Maillard to arrive at the novel and unobvious combination of elements recited in the claimed invention, and further, that the Examiner has not established a reasonable basis for such combination of Leppek and Maillard, for several reasons.

As the Examiner well knows, merely identifying the individual elements of the claims in separate references is not sufficient to establish the obviousness of the claims. The Office Action must establish a reasonable motivation or suggestion, in the references themselves or in the art in general, for combining the references to arrive at the claimed invention.

The mere fact that references could (or can) be combined or modified is not sufficient to establish *prima facie* obviousness (see M.P.E.P. § 2143.01). There must be a reasonable motivation to do that which the patent applicant has done.

In this case, the Examiner appears to be using circular logic to rely on Leppek for disclosing the features of the claimed invention, with reference to a smart card, but then acknowledges that Leppek does not disclose such a smart card.

On the other hand, the Examiner merely cites Maillard, which does disclose a smart card, as being combinable with the Leppek reference in order to arrive at the claimed invention.

However, Applicants respectfully submit that the Examiner has not explained, nor do the reference provide support for, *how* the features relied upon in Leppek, which is *not* a smart card, could (or would) be implemented in a smart card, such as the smart card of Maillard, or for that matter, how such a combination would arrive at the claimed invention.

That is, it is not enough merely to identify the individual elements of the claims in separate references to establish the obviousness of the claimed invention. The Office Action must establish a reasonable motivation or suggestion, in the references themselves or in the art in general, for combining the references to arrive at the claimed invention.

Moreover, Applicants respectfully submit that the Examiner has not established a reasonable motivation for such a combination and/or modification.

That is, Applicants respectfully submit that merely alleging that it would have been obvious to implement the teachings of Leppek onto a smart card "*because smart cards are small, easy to use mediums for encryption*" and because "*a method which prevents a footprint or playback attack (sic) from being performed by an intruder would help spread the acceptance of smart cards used in technology*" is not sufficient to establish a reasonable motivation for combining the references to arrive at the claimed invention.

On the contrary, the Office Action must establish a reasonable motivation or suggestion, in the references themselves or in the art in general, for combining the references to arrive at the claimed invention.

Absent a reasonable motivation, it would appear that the Examiner is using improper hindsight based analysis to arrive at the claimed invention,

Thus, for at least the foregoing reasons, Applicants respectfully submit that it would not have been obvious to combine Leppek and Maillard to arrive at the claimed invention, absent impermissible hindsight based analysis.

Moreover, even assuming *arguendo* that it would have been obvious to combine Leppek and Maillard, Applicants respectfully submit that such a combination still would not arrive at the claimed invention.

For example, Leppek teaches using a plurality of secret encryption schemes managed in an "encryption operators database". The idea in Leppek is that most likely the attacker (e.g., the intruder, counterfeiter, etc.) or would not know all encryption operators in the database, nor be able to recognize which one is being used to protect some data set in a given communication.

Particularly, Leppek discloses a "virtual" encryption scheme that combines selected ones of a plurality of different encryption operators stored in an encryption operator database into a compound sequence of encryption operators. Data to be transported from a data source site, such as a user workstation, to a destination or data recipient site, is sequentially encrypted by performing a compound sequential data flow through this sequence prior to transmission (e.g., see Leppek at Abstract).

In other words, Leppek is concerned with trying to protect the secret of (within) messages.

Applicants respectfully submit that this sort of combination of encryption scheme is in fact well known (and is the typical sort of ideas everyone thinks about early on when exposed to the issues of cryptography). Such encryption schemes are usually considered as potentially dangerous among cryptographers, who generally prefer more solid, simple algorithms to complex combinations that may prevent effective testing of the strength of the protection, while creating an illusory sentiment of an acceptable safety level.

In comparison, in the claimed invention, rather than trying to protect the secret of (within) messages, the claimed invention authenticates or authorizes the smart cards that are built according to the claimed invention.

Thus, the present invention is of a very different nature than Leppek, which is unrelated to smart cards.

For example, the present invention uses original, but simple protocols based on the best controlled encryption/signature technologies, so that the efficiency of the present invention readily can be assessed by any expert.

Contrary to Leppek or Maillard, the claimed invention provides protection for a smart card on top of (i.e., in addition to) rather widely known technologies and practices, such as those in Leppek, or for that matter, in Maillard.

As described by Applicants, smart cards have been proposed as a technology offering the possibility of secure off-line transactions (e.g., see specification at page 1, lines 8-9). However, recently, several successful attacks on conventional smart cards have been reported (e.g., see specification at page 1, lines 10-14).

The claimed invention, however, provides a solution to well defined problems of the smart card industry.

For example, independent claim 1 recites a method of preventing counterfeiting of a smart card, comprising:

> providing a smart card with a cryptographic structure *for authorizing the smart card* which cannot be accessed completely by a predetermined small number of readings,
> wherein said cryptographic structure can be built only by whoever emits the card or an agent thereof (emphasis added).

On the other hand, independent claim 24 recites a method of preventing counterfeiting of a smart card, comprising:

> providing a smart card such that none of confidential information and a cryptographic key *for authorizing the smart card*, is carried on the smart card;
> reading said card by a reader such that in each reading, said reader reads only a predetermined small amount of information which makes the card unique

Further, independent claim 27 recites a signal-bearing medium tangibly embodying a program of machine-readable instructions executable by a digital processing apparatus to perform a method for preventing counterfeiting and cloning of smart cards, comprising:

> providing a smart card with a cryptographic structure *for authorizing the smart card* which cannot be accessed completely by a predetermined number of readings,
> wherein said cryptographic structure can be built only by whoever emits the card or an agent thereof.

As mentioned above, the claimed invention, as defined by independent claims 1, 24, and 27, does not merely protect the secret of messages, but instead, authenticates or authorizes the smart cards that are built according to the claimed invention.

Thus, Applicants respectfully submit that there is a clear and profound difference between the cited references and the claimed invention.

Accordingly, Applicants respectfully submit that it clearly would not have been obvious to the ordinarily skilled artisan to combine and modify Leppek and Maillard, which are vaguely related references, to arrive at the novel and unobvious features of the claimed invention.

Thus, for the foregoing reasons, Applicants respectfully submit that neither Leppek nor Maillard, alone or in combination, discloses or suggests all of the features of claims 1, 3-7, 9, 13, 24, 25, and 27, and therefore, respectfully requests that the Examiner with draw this rejection.

B. Claims 2, 10-12, 14, 23, and 26 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Leppek in view of Maillard, and further in view of Perlman. Applicant submits, however, that there are elements of the claimed invention which are neither taught nor suggested by Leppek, Maillard, or Perlman, alone or in combination, and therefore, Applicants respectfully traverse this rejection.

Applicants respectfully submit that Perlman does not make up for the deficiencies of Leppek and Maillard, as set forth above.

Therefore, Applicants submit that claims 2, 10-12, 14, and 23 are patentable over Leppek, Maillard, or Perlman, alone or in combination, at least by virtue of their dependency from independent claim 1.

For somewhat similar reasons, Applicants respectfully submit that neither Leppek, Maillard, nor Perlman, either alone or in combination, discloses or suggests the novel and unobvious combination of features recited in independent claim 26.

For example, independent claim 26 recites a system for preventing cloning of a smart card, comprising:

> a smart card such that a cryptographic structure for authorizing the smart card is not carried on the smart card; and
> a reader for reading the smart card and including a database for linking to a network and being updated periodically with a list of unauthorized smart cards,
> wherein said cryptographic structure is kept secret by whoever emits the card or an agent thereof.

As mentioned above, the claimed invention, as defined by independent claim 26, does not merely protect the secret of messages, but instead, authenticates or authorizes the smart cards that are built according to the claimed invention. As such, Applicants respectfully submit that there is a clear and profound difference between the cited references and the claimed invention.

Thus, for the foregoing reasons, Applicants respectfully submit that neither Leppek, Maillard, nor Perlman, alone or in combination, discloses or suggests all of the features of claims 2, 10-12, 14, 23, and 26, and therefore, respectfully requests that the Examiner with draw this rejection.

C. Claims 8, 15-18, and 20-22 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Leppek in view of Maillard, and further in view of Schneier.

Applicants respectfully submit that Schneier does not make up for the deficiencies of Leppek and Maillard, as set forth above.

Therefore, Applicants submit that claims 8, 15-18, and 20-22 are patentable over Leppek, Maillard, or Schneier, alone or in combination, at least by virtue of their dependency from independent claim 1.

Thus, for the foregoing reasons, Applicants respectfully submit that neither Leppek, Maillard, nor Schneier, alone or in combination, discloses or suggests all of the features of claims 8, 15-18, and 20-22, and therefore, respectfully requests that the Examiner with draw this rejection.

D. Claim 19 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Leppek in view of Maillard, and further in view of Schneier, and further in view of Perlman.

Applicants respectfully submit that Schneier does not make up for the deficiencies of Leppek, Maillard, or Perlman, as set forth above.

Therefore, Applicants submit that claim 19 is patentable over Leppek, Maillard, Perlman, or Schneier, alone or in combination, at least by virtue of its dependency from independent claim 1.

Thus, for the foregoing reasons, Applicants respectfully submit that neither Leppek, Maillard, Schneier, nor Perlman, alone or in combination, discloses or suggests all of the features of claim 19, and therefore, respectfully requests that the Examiner with draw this rejection.

III. CONCLUSION

The specification and claims have been amended herewith to obviate the objections to the drawings, specification, and claims, and therefore, the Examiner respectfully is requested to withdraw these objections.

In view of the foregoing, Applicant submits that claims 1-27, all the claims presently pending in the application, are patentably distinct over the prior art of record and are in condition for allowance. The Examiner is respectfully requested to pass the above application to issue at the earliest possible time.

Should the Examiner find the application to be other than in condition for allowance, the Examiner is requested to contact the undersigned at the local telephone number listed below to discuss any other changes deemed necessary in a telephonic or personal interview.

The Commissioner is hereby authorized to charge any deficiency in fees or to credit any overpayment in fees to Assignee's Deposit Account No. 50-0510.

Respectfully Submitted,

Date: July 1, 2004

John J. Dresch, Esq.
Registration No. 46,672

Sean M. McGinn, Esq.
Registration No. 34,386

McGinn & Gibb, PLLC
8321 Old Courthouse Road, Suite 200
Vienna, VA 22182-3817
(703) 761-4100
Customer No. 21254